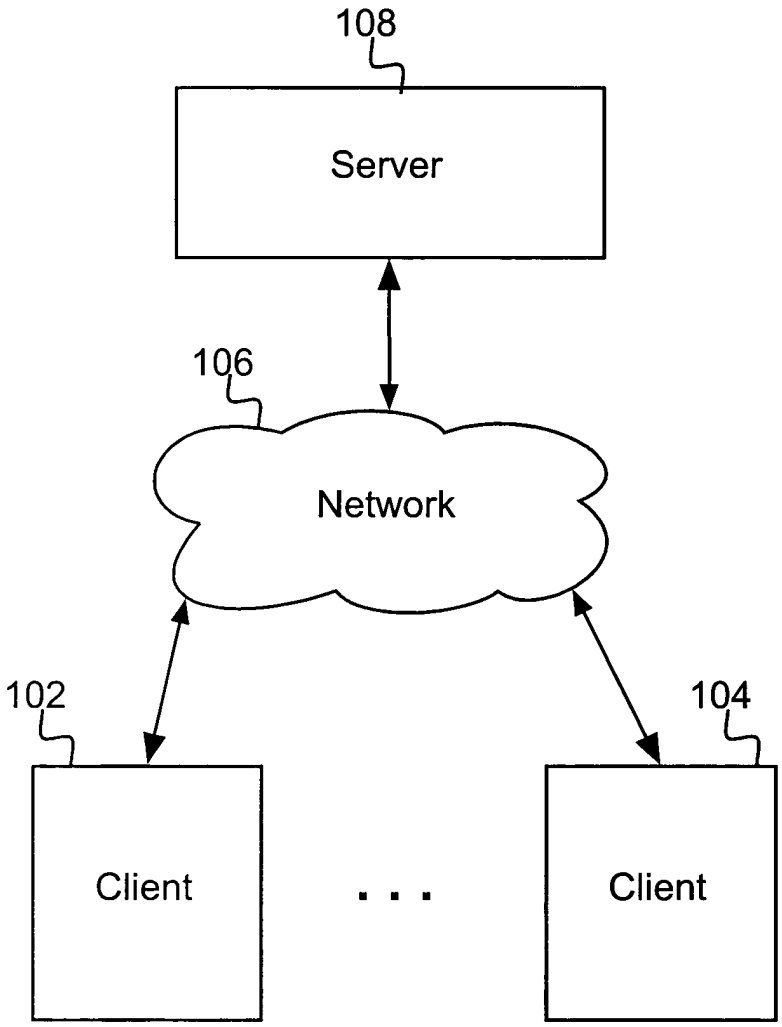

FIG. 1

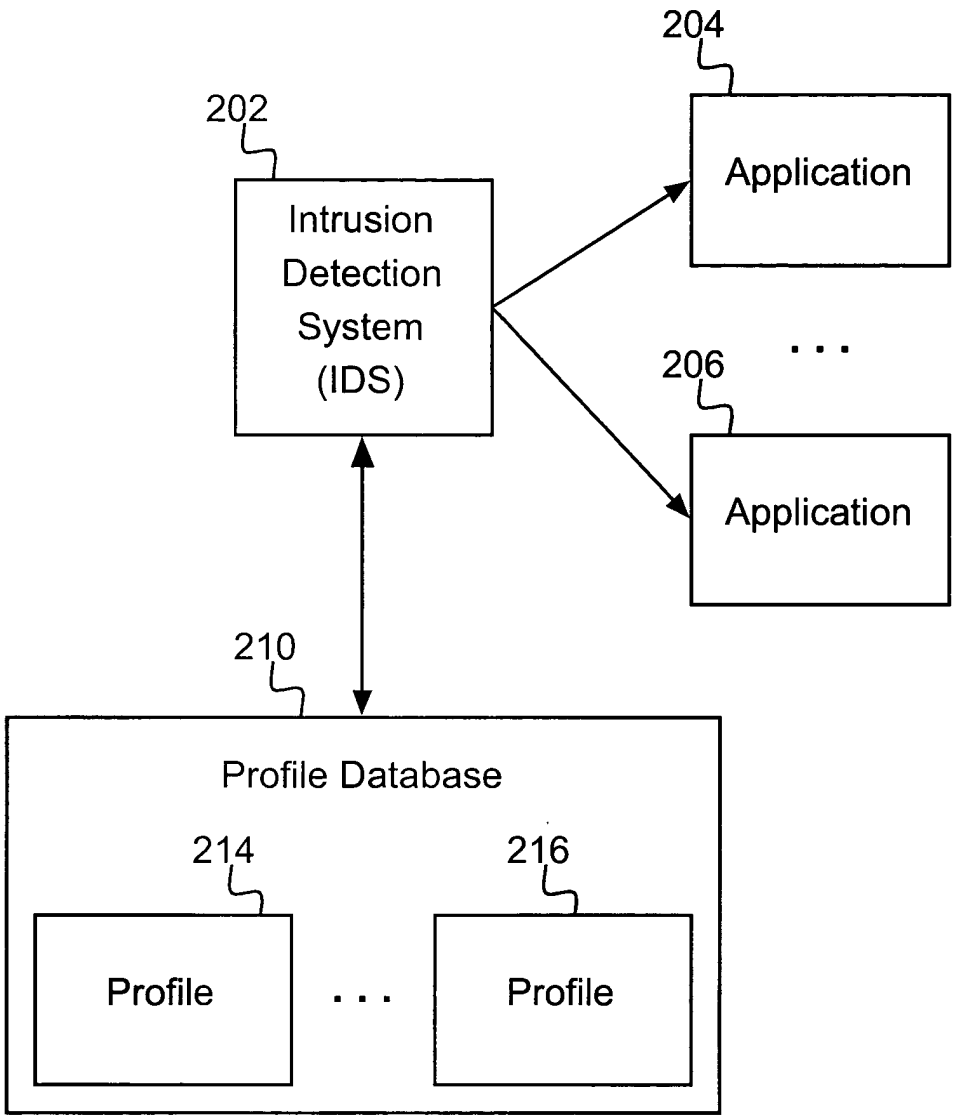
204
202
Application
Intrusion
Detection
System
(IDS)
206
Application
210
Profile Database
214
216
Profile
Profile

FIG. 2

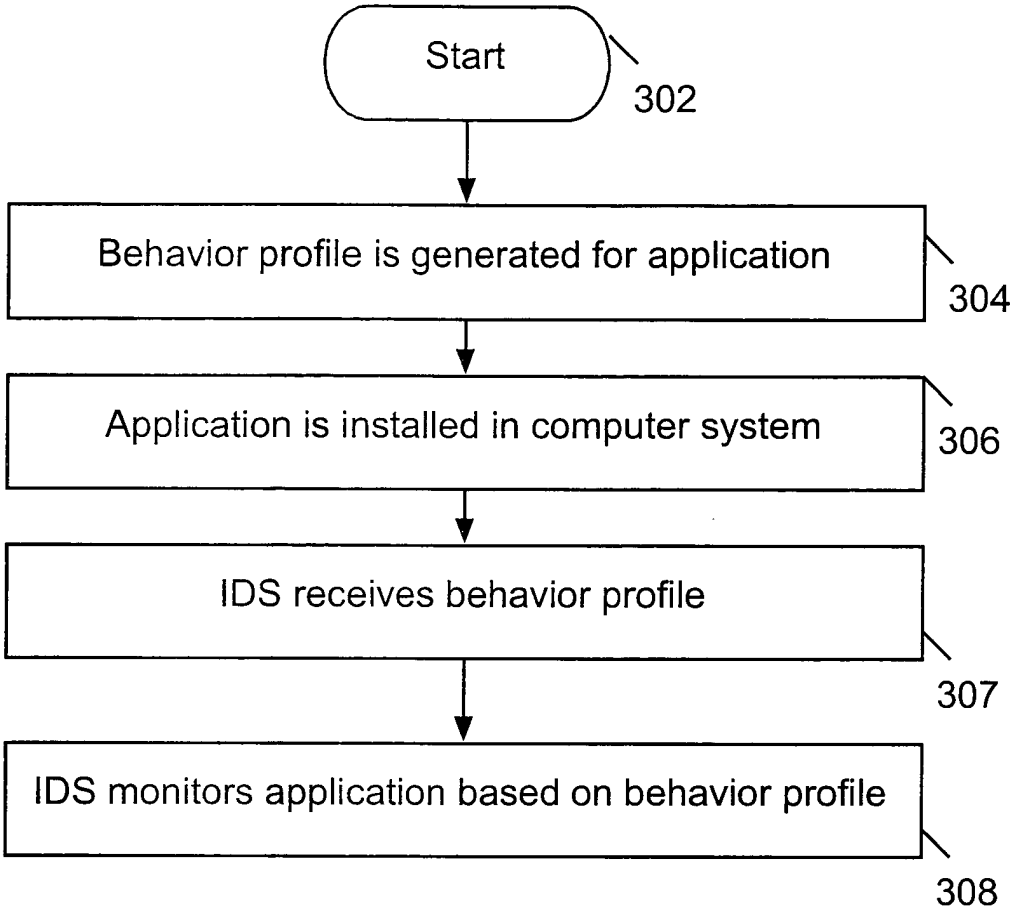
Start
302
Behavior profile is generated for application
304
Application is installed in computer system
306
IDS receives behavior profile
307
IDS monitors application based on behavior profile
308

FIG. 3

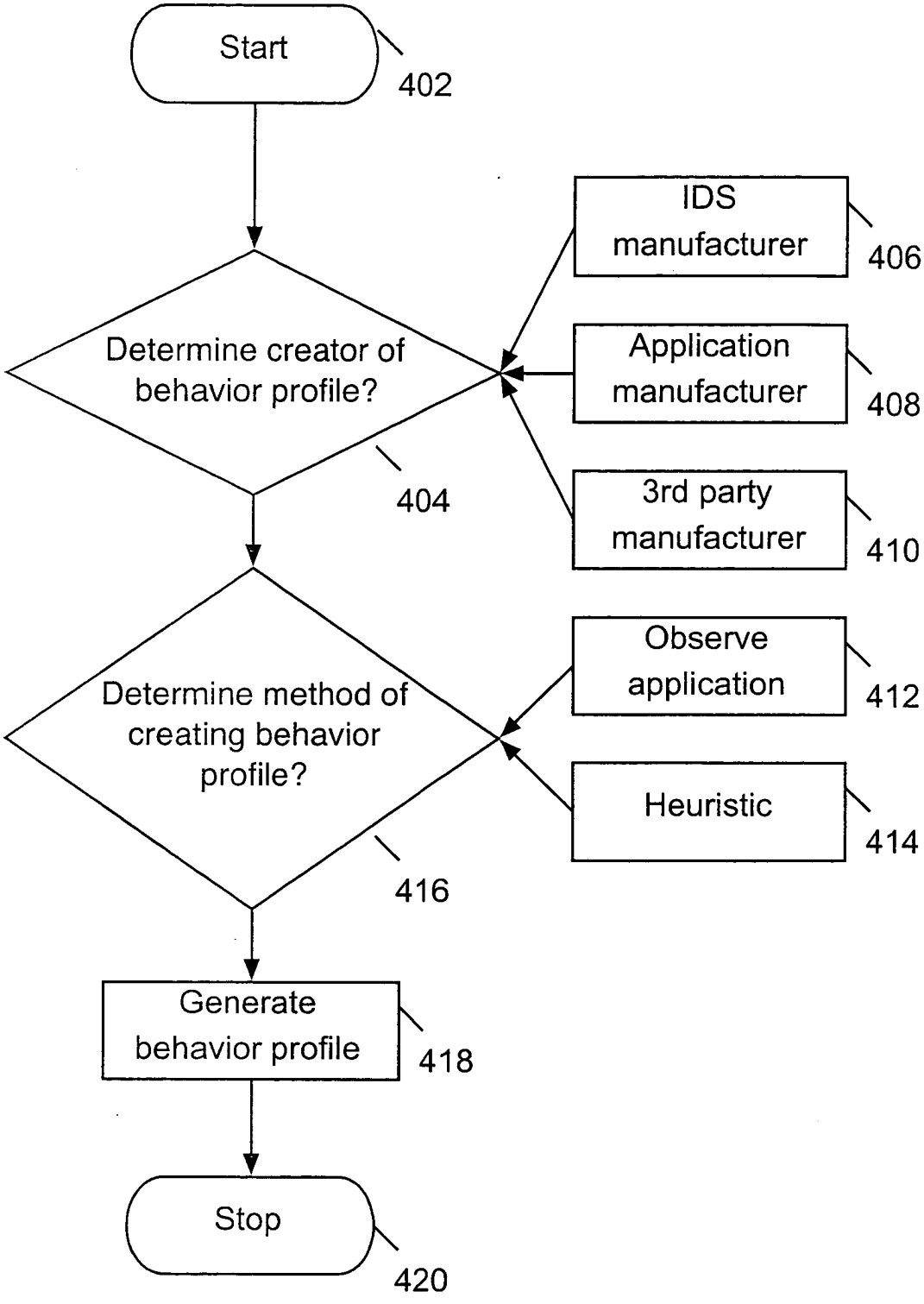
Start
402
IDS manufacturer
406
Determine creator of behavior profile?
Application manufacturer
408
404
3rd party manufacturer
410
Determine method of creating behavior profile?
Observe application
412
Heuristic
414
416
Generate behavior profile
418
Stop
420

FIG. 4

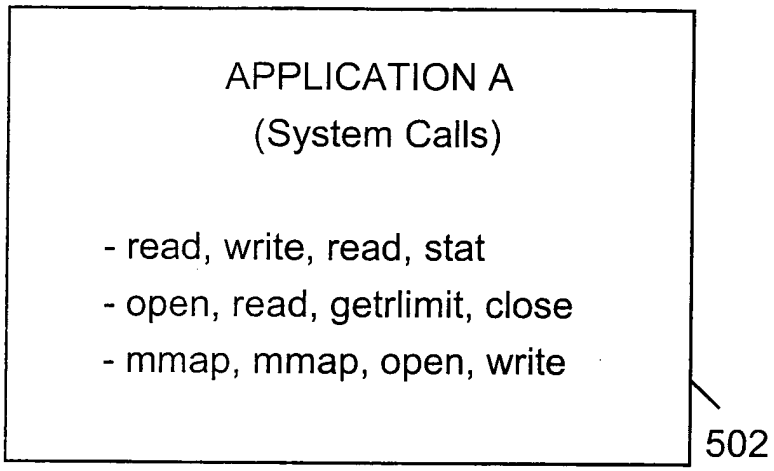
APPLICATION A
(System Calls)
- read, write, read, stat
- open, read, getrlimit, close
- mmap, mmap, open, write
502

FIG. 5

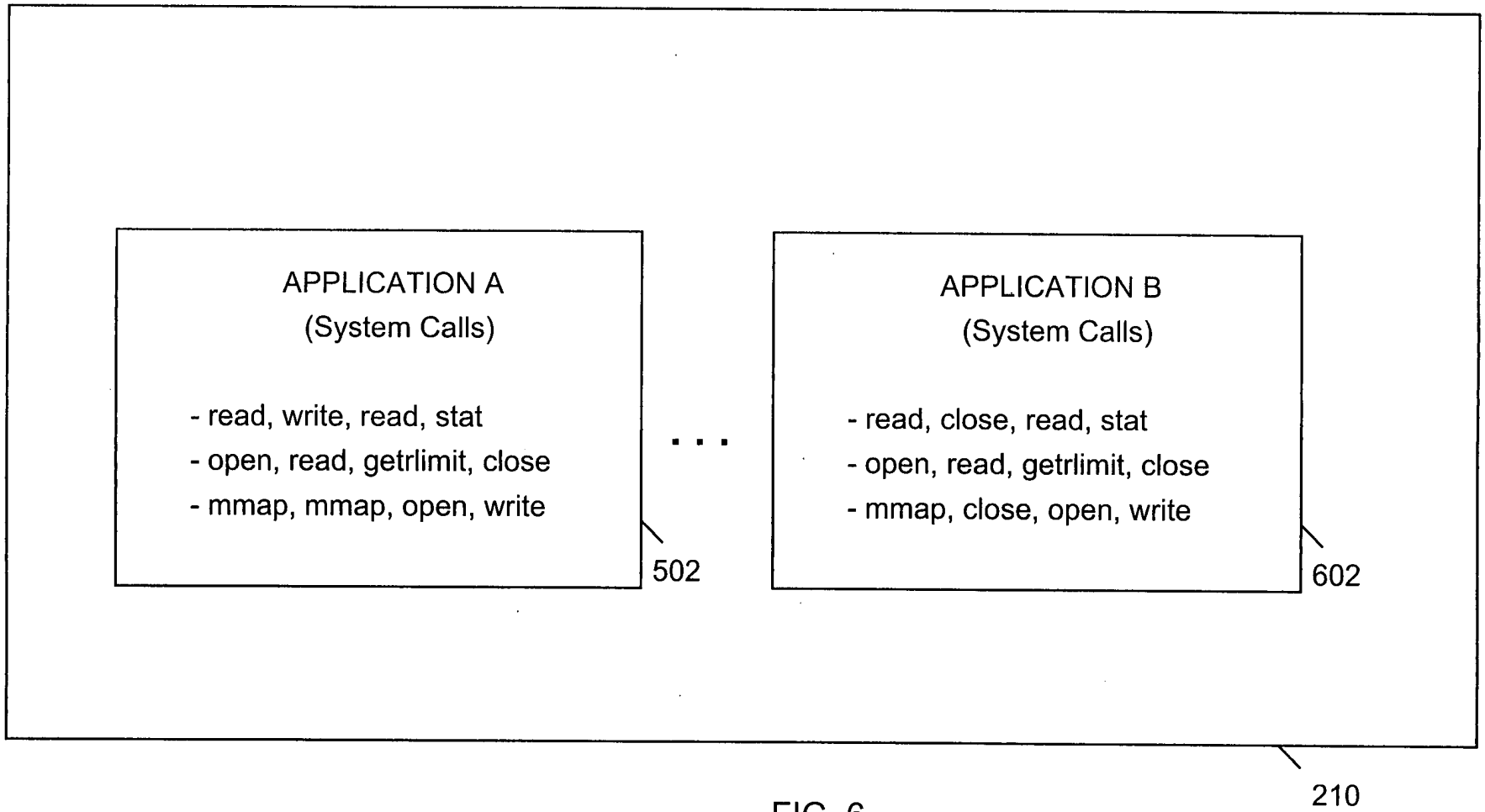
APPLICATION A
(System Calls)
- read, write, read, stat
- open, read, getrlimit, close
- mmap, mmap, open, write
502
APPLICATION B
(System Calls)
- read, close, read, stat
- open, read, getrlimit, close
- mmap, close, open, write
602
210

FIG. 6

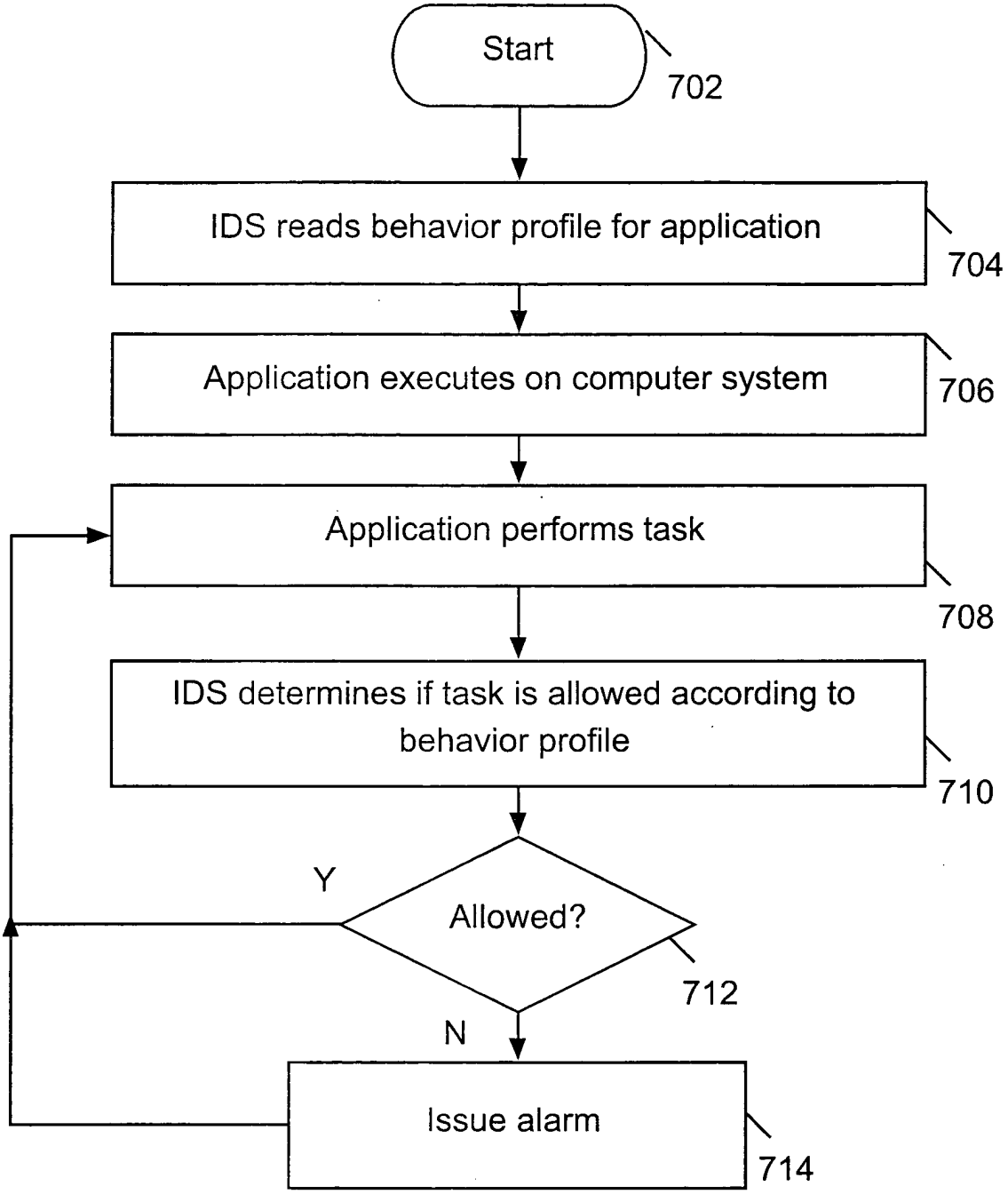
Start
702
IDS reads behavior profile for application
704
Application executes on computer system
706
Application performs task
708
IDS determines if task is allowed according to behavior profile
710
Y
Allowed?
712
N
Issue alarm
714

FIG. 7

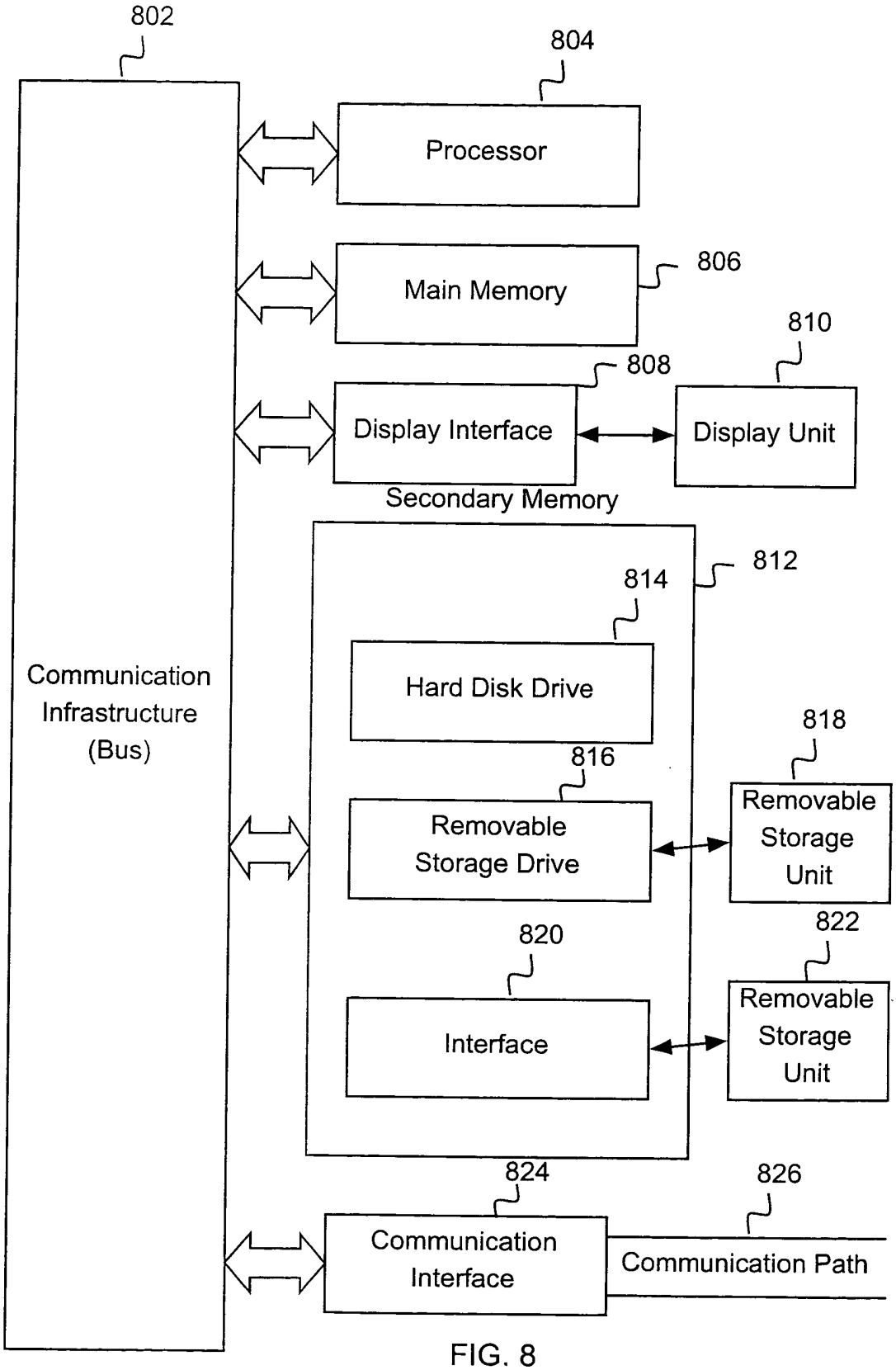
802
804
Processor
Main Memory
806
810
808
Display Interface
Display Unit
Secondary Memory
812
814
Hard Disk Drive
Communication Infrastructure (Bus)
818
816
Removable Storage Drive
Removable Storage Unit
822
820
Interface
Removable Storage Unit
824
826
Communication Interface
Communication Path

FIG. 8